Secure Registration for a Multicast-Broadcast-Multimedia System (MBMS)

BACKGROUND

Field of the Invention

[1001] The present invention relates generally to telecommunications, and more specifically, to security in communication systems.

Background

[1002] In a wireless communication system which carries non-voice traffic, such as video, data, multimedia, or other types of traffic in addition to voice traffic, a typical cellular base station may broadcast a multimedia traffic service if the number of users demanding the service exceeds a predetermined threshold number within the coverage area of the base station. The multimedia traffic service may be a video stream of an event such as a sporting event or a highlighted portion of a sporting event, for example. If there are not enough users demanding the service in the coverage area, the base station may transmit the service only to the specific users who have demanded the service through dedicated channels instead of broadcasting the service to all users in the coverage area.

[1003] Sometimes a rogue or illegitimate user may attempt to force the base station to broadcast the service to all

users in the coverage area by registering multiple times in an idle mode, for example, by assuming a number of different identities. If one or more rogue users use mobile telephones in the idle mode to register multiple times in a coverage area to receive the contents of an event, the base station may count the number of registrations as legitimate user registrations for the event and broadcast the event to all users in the coverage area.

[1004] Therefore, there is a need in the art for a network operator or content provider to have reliable means to verify that only legitimate registrations for a multimedia event be counted in a coverage area and not be forced to broadcast the event to all users in the coverage area due to fake registrations.

SUMMARY

[1005] Embodiments disclosed herein address the above stated needs by a method and an apparatus of obtaining secure registration in a multicast-broadcast-multimedia system (MBMS) using a temporary registration key (RGK).

BRIEF DESCRIPTION OF THE DRAWINGS

[1006] FIG. 1 is an exemplary block diagram illustrating a multicast-broadcast-multimedia system (MBMS) communication link;

[1007] FIG. 2 is a diagram illustrating an embodiment of secure registration in the MBMS; and

[1008] FIG. 3 is a diagram illustrating another embodiment of secure registration in the MBMS.

DETAILED DESCRIPTION

[1009] The word "exemplary" is used herein to mean "serving as an example, instance, or illustration." Any embodiment described herein as "exemplary" is not necessarily to be construed as preferred or advantageous over other embodiments. All of the embodiments described in this Detailed Description are exemplary embodiments provided to enable persons skilled in the art to make or use the invention and not to limit the scope of the invention which is defined by the claims.

[1010] A mobile station, also called user equipment (UE), may communicate with one or more base stations. A mobile station transmits and receives data packets through one or more base stations to a base station controller. Base stations and base station controllers are parts of a network called an access network. An access network transports data packets between multiple mobile stations. The access network may be further connected to additional networks outside the access network, such as a corporate intranet or the Internet, and may transport data packets between each mobile station and such outside networks. A

mobile station that has established an active traffic channel connection with one or more base stations is called an active mobile station, and is said to be in a traffic state. A mobile station that is in the process of establishing an active traffic channel connection with one or more base stations is said to be in a connection setup state. A mobile station that is powered on and capable of receiving signals from a base station but is not in a traffic state or in a connection setup state is said to be in an idle state.

[1011] A communication link through which a mobile station sends signals to a base station is called a reverse link. A communication link through which a base station sends signals to a mobile station is called a forward link. A mobile station or user equipment (UE) may be a mobile telephone which includes a mobile telephone handset, also called mobile equipment (ME), and a memory module, such as a physically secure integrated circuit card or smart card called UICC, which may be removable or permanently attached to the ME. In a Global System for Mobile communication (GSM) telephone, the UICC is typically a subscriber identity module (SIM). In a code division multiple access (CDMA) telephone, the UICC is typically a removable user identity module (RUIM).

[1012] FIG. 1 is an exemplary block diagram illustrating a communication link between user equipment (UE) 2, a serving

network 4, a home network 6 and a content provider (CP) 8 in a multicast-broadcast-multimedia system (MBMS). The user equipment 2 may be a mobile station which includes mobile equipment (ME) 10 and a memory module or UICC 12. The UICC 12 may be either a removable memory module attached to the mobile equipment 10 or a permanent part of the mobile equipment 10. The physical implementation of the UICC 12 in the user equipment 2 is not critical to the present invention.

[1013] The serving network 4 may either be owned by the wireless carrier which provides subscription service to the user equipment 2, or be a visited network owned by another carrier which provides service to the user equipment 2 while the user equipment 2 is roaming. The serving network 4 typically includes a radio access network (RAN) 14 and a serving general packet radio service (GPRS) support node (SGSN) 16. The radio access network 14, also known as a base station (BS), a base transceiver station (BTS), or an access point (AP), transmits radio signals to and receives radio signals from the user equipment 2. The SGSN 16 is a core network node which may be part of a public land mobile network (PLMN), for example.

[1014] The home network 6 is the network owned by the wireless carrier which provides subscription service to the user equipment 2, and may or may not be owned by the same carrier as that of the serving network 4 depending upon

whether the user equipment 2 is roaming outside the service area of the carrier. The home network 6 typically includes a gateway GPRS support node (GGSN) 18, a broadcast-multicast-service center (BM-SC) 20 and a home subscriber server (HSS) 22. The solid line 22 in FIG. 1 represents a bearer path on which information-bearing signals are carried from the content provider 8 through the home network 6 and the serving network 4 to the mobile equipment 10. The dashed line 24 in FIG. 1 represents a key/authorization path on which encryption and decryption keys are passed between the UICC 12, the serving network 4 and the home network 6.

[1015] The content provider 8 may be a third-party content source that is owned by neither the home network carrier nor the serving network carrier. The home subscriber server 22 in the home network 6 may include a database for holding mobile telephone subscription and collecting billing data for multicast services. In the embodiment shown in FIG. 1, the home network 6 also includes the broadcast-multicast-service center (BM-SC) 20 which schedules multicasting of the multimedia event and performs at least some security functions for the MBMS. The serving network 4 is the network that transmits the content to a single user through a dedicated channel, multicasts the content to a plurality of users through dedicated channels if the number of users demanding the service does not

justify broadcasting the service to all users in the coverage area, or broadcasts the content to all users in the coverage area if the number of users demanding the service exceeds a predetermined threshold.

[1016] In an embodiment, the content of the multimedia event is encrypted and decrypted in the multicast-broadcast-multimedia system through several levels of encryption and decryption to provide at least some level of assurance that unauthorized users will not be able to decrypt the data and watch the multimedia event. For example, a permanent, user-specific registration key (RK) may be provided to generate temporary key (TK) values and to authenticate the UICC in the user's mobile telephone. The TK is a single use, user-specific key used to encrypt broadcast access key (BAK) values. The TK is also used by the UICC to decrypt the BAK values. The BAK is a medium-term, shared key which is used for deriving multiple short-term keys (SK) and distributed to UICCs of subscribed users on a per-user basis. The SK is a frequently changing, shared key which is used to encrypt and decrypt the content. The SK may be generated using a random number (SK_RAND) which is sent in the clear with the encrypted content and the BAK. The UICC 12 regenerates the SK from the BAK and SK_RAND, and passes the SK to the mobile equipment 10. Examples of schemes for encryption and decryption of data contents in a multicast-broadcast-

multimedia system are described in U.S. Patent Application Serial No. 09/933,972, entitled "Method and Apparatus for Security in a Data Processing System," filed August 20, 2001, incorporated herein by reference. Various other embodiments of using public keys or shared-secret keys for encryption and decryption may also be implemented within the scope of the invention. For example, in an alternate embodiment, secure delivery or provisioning of BAK to the UICC may be provided by using public key mechanisms such as RSA or ElGamal, which are known to persons skilled in the art.

[1017] FIG. 2 illustrates an embodiment of secure registration in a multicast-broadcast-multimedia system. In this embodiment, the broadcast-multicast-service center (BM-SC) 20 transmits a provisioning message, which is a function of a public land mobile network (PLMN) key referred to as PK, and the permanent, user-specific registration key referred to as RK. The PK is a temporary, home PLMN specific key used to generate a radio access network (RAN) key referred to as RAK, and to authenticate the UICC 12. The provisioning message is transmitted from the BM-SC 20 to the UICC 12 along a path 26 as illustrated in FIG. 2. The provisioning message, which is a function with arguments PK and RK, may be represented as c1(PK, RK). Upon receiving the provisioning message, the UICC 12 extracts the PK from the provisioning message and stores

the PK value. Other embodiments for implementing the secure delivery or provisioning of PK to the UICC may be provided within the scope of the invention by using public key mechanisms including but not limited to RSA and ElGamal.

[1018] The radio access network (RAN) 14 transmits a request for the RAK and a random number (RAND) along a path 28 to the BM-SC 20, which in response generates the RAK which is a function with arguments PK and RAND. The RAK, which may be represented as c2(PK, RAND), is transmitted by the BM-SC 20 to the RAN 14 along a path 30. The RAK is a temporary, RAN specific key used to generate temporary, user-specific registration key (RGK) values and to hide the PK from the RAN 14 which is visited by the UE 2. The RAK is also used to cipher the MBMS service identification number (Serv_ID) and a user identification number such as P-TMSI, IMSI, electronic serial number (ESN), MIN, or any permanent or temporary user identification number used in the system in which an embodiment of the present invention is implemented. In the embodiments shown in FIGs. 2 and 3, P-TMSI is used as an exemplary user identification number known to a person skilled in the art.

[1019] The RAN may store the RAK and broadcast the RAND to all users including UE 2 within the coverage area of the RAN along a path 32. The UE 2, upon receiving the RAND, sends the RAND as well as the P-TMSI and the Serv_ID to the

UICC 12 along a path 34. The UICC 12 generates the RAK which is an exact copy of the RAK generated by the BM-SC 20. After receiving the Serv_ID and the P-TMSI, the UICC 12 concatenates the Serv_ID and the P-TMSI to obtain a concatenated result denoted as [Serv_ID||P-TMSI], and computes a cyclic redundancy code (CRC) based on the Serv_ID and P-TMSI. The CRC is appended to [Serv_ID||P-TMSI] to generate [Serv_ID||P-TMSI||CRC]. The UICC 12 then generates the RGK which is a function of the Serv_ID, P-TMSI, CRC and RAK represented as c3([Serv_ID||P-TMSI||CRC], RAK). The RGK is a temporary, user-specific key used to authenticate registration messages.

[1020] After the RGK is generated, the UICC 12 sends the RGK along a path 36 to the UE 2, which in turn transmits a registration/connection request including the RGK to the RAN 14 along a path 38. The RAN 14, upon receiving the registration/connection request, extracts the [Serv_ID||P-TMSI], verifies the CRC, and counts the user identified by the P-TMSI as a legitimate user who has sent a valid registration message to request the multimedia service. If the registration/connection message transmitted by the user is not verified by the RAN 14, then the RAN may regard the user as a rogue or illegitimate user and does not count the request as legitimate.

[1021] FIG. 3 illustrates another embodiment of secure registration in a multicast-broadcast-multimedia system.

In this embodiment, no provisioning message is transmitted by the broadcast-multicast-service center (BM-SC) 20. Instead, the radio access network (RAN) 14 transmits a request for the RAK and a random number (RAND) along a path 40 to the BM-SC 20, which in response generates the RAK and the RAND. The RAK is a function with arguments BAK and RAND represented as c2(BAK, RAND). The BAK is the same broadcast access key used as part of the encryption scheme to encrypt the data contents described above. The RAND and RAK are transmitted by the BM-SC 20 to the RAN 14 along a path 42. The RAK is a temporary, RAN specific key used to generate temporary, user-specific registration key (RGK) values. The RAK is also used to cipher the MBMS service identification number (Serv_ID) and a user identification number referred to as P-TMSI.

[1022] The RAN may store the RAK and broadcast the RAND to all users including UE 2 within the coverage area of the RAN along a path 44. The UE 2, upon receiving the RAND, sends the RAND as well as the P-TMSI and the Serv_ID to the UICC 12 along a path 46. The UICC 12 generates the RAK which is an exact copy of the RAK generated by the BM-SC 20. After receiving the Serv_ID and the P-TMSI, the UICC 12 concatenates the Serv_ID and the P-TMSI to obtain a concatenated result denoted as [Serv_ID||P-TMSI], and computes a cyclic redundancy code (CRC) based on the Serv_ID and P-TMSI. The CRC is appended to [Serv_ID||P-

TMSI] to generate [Serv_ID||P-TMSI||CRC]. The UICC 12 then generates the RGK which is a function of the Serv_ID, P-TMSI, CRC and RAK, represented as c3([Serv_ID||P-TMSI||CRC], RAK). The RGK is a temporary, user-specific key used to authenticate registration messages.

[1023] After the RGK is generated, the UICC 12 sends the RGK along a path 48 to the UE 2, which in turn transmits a registration/connection request including the RGK to the RAN 14 along a path 50. The RAN 14, upon receiving the registration/connection request, extracts the [Serv_ID||P-TMSI], verifies the CRC, and counts the user identified by the P-TMSI as a legitimate user who has sent a valid registration message to request the multimedia service. If the registration/connection message transmitted by the user is not verified by the RAN 14, then the RAN may regard the user as a rogue or illegitimate user and does not count the request as legitimate.

[1024] The RAN 14 may receive a plurality of registration/connection requests from a plurality of users within the coverage area and decide which requests are valid ones transmitted by legitimate users by verifying the CRC computed from the Serv_ID and P-TMSI of each user. The RAN may ignore those requests with RGKs which include unverifiable CRCs. In this manner, the RAN has a highly reliable means of determining how many registration requests for a certain multimedia event are valid, and

would not be forced to broadcast the event if the number of legitimate users is not enough to justify broadcasting the event.

[1025] Various other features may also be added to the temporary registration message (RGK) within the scope of the present invention. For example, a time stamp for system time may be added to the RGK. The RAN 14 may use the P-TMSI extracted from the RGK to determine whether the user who is attempting to register is actually a subscriber, if the RAN has the P-TMSIs of all subscribed users in the coverage area. In a typical GSM system, the P-TMSI may be allocated at the logical link control (LLC) level in the GSM/GPRS, that is, in the core network (CN). In another embodiment, a public key may be used in forming the RGK to avoid replay attacks by rogue users. For example, if each UICC has a private key used for provisioning PK or BAK, the RGK may include a reference to the public key or certificate and a signature of the BAK-hash or PK-hash. Replay attacks by rogue users may be prevented or at least limited by using techniques such as sequence numbers or digital signatures based on public key cryptography.

[1026] The sequence of the text in any of the claims does not imply that process steps must be performed in a temporal or logical order according to such sequence unless it is specifically defined by the language of the claim.

The process steps may be interchanged in any order without departing from the scope of the invention as long as such an interchange does not contradict the claim language and is not logically nonsensical. Furthermore, numerical ordinals such as "first," "second," "third," etc. simply denote different singles of a plurality and do not imply any order or sequence unless specifically defined by the claim language.

[1027] Furthermore, words such as "connect," "connected to" and "connection" used in describing a relationship between different elements do not imply that a direct physical connection must be made between these elements. For example, two elements may be connected to each other physically, electronically, logically, or in any other manner, through one or more additional elements, without departing from the scope of the invention.

[1028] Those of skill in the art would understand that information and signals may be represented using any of a variety of different technologies and techniques. For example, data, instructions, commands, information, signals, bits, symbols, and chips that may be referenced throughout the above description may be represented by voltages, currents, electromagnetic waves, magnetic fields or particles, optical fields or particles, or any combination thereof.

[1029] Those of skill would further appreciate that the various illustrative logical blocks, modules, circuits, and algorithm steps described in connection with the embodiments disclosed herein may be implemented as electronic hardware, computer software, or combinations of both. To clearly illustrate this interchangeability of hardware and software, various illustrative components, blocks, modules, circuits, and steps have been described above generally in terms of their functionality. Whether such functionality is implemented as hardware or software depends upon the particular application and design constraints imposed on the overall system. Skilled artisans may implement the described functionality in varying ways for each particular application, but such implementation decisions should not be interpreted as causing a departure from the scope of the present invention.

[1030] The various illustrative logical blocks, modules, and circuits described in connection with the embodiments disclosed herein may be implemented or performed with a general purpose processor, a digital signal processor (DSP), an application specific integrated circuit (ASIC), a field programmable gate array (FPGA) or other programmable logic device, discrete gate or transistor logic, discrete hardware components, or any combination thereof designed to perform the functions described herein. A general purpose

processor may be a microprocessor, but in the alternative, the processor may be any conventional processor, controller, microcontroller, or state machine. A processor may also be implemented as a combination of computing devices, e.g., a combination of a DSP and a microprocessor, a plurality of microprocessors, one or more microprocessors in conjunction with a DSP core, or any other such configuration.

[1031] The steps of a method or algorithm described in connection with the embodiments disclosed herein may be embodied directly in hardware, in a software module executed by a processor, or in a combination of the two. A software module may reside in random access memory (RAM), flash memory, read only memory (ROM), erasable programmable read only memory (EPROM), electrically erasable programmable read only memory (EEPROM), registers, a hard disk, a removable disk, a compact disc-read only memory (CD-ROM), or any other form of storage medium known in the art. An exemplary storage medium is coupled to the processor such that the processor can read information from, and write information to, the storage medium. Alternatively, the storage medium may be integral to the processor. The processor and the storage medium may reside in a single ASIC or as separate components in a base station, for example.

[1032] The previous description of the disclosed embodiments is provided to enable any person skilled in the art to make or use the present invention. Various modifications to these embodiments will be readily apparent to those skilled in the art, and the generic principles defined herein may be applied to other embodiments without departing from the spirit or scope of the invention. Thus, the present invention is not intended to be limited to the embodiments shown herein but is to be accorded the widest scope consistent with the principles and novel features disclosed herein.

WHAT IS CLAIMED IS: